SECTION 16.3

RESTRICTING ACCESS TO PERSONAL INFORMATION

Essential Question

What is the importance of restricting access to your personal information to your financial success?

Personal information should be protected as if it is as important as money. Social Security, credit card, and bank and utility account numbers can be used by cyber criminals to steal money, open new accounts, or open fraudulent credit lines. This information should not be handed out to anyone.

Each time you are asked for personal information, decide whether the requester is valid. Remember that scammers will often do anything they can to gain trust. Requests for personal information may come from web forms, e-mails, text messages, or phone calls. This section discusses how to restrict access to personal information.

Monkey Business Images/Shutterstock.com

LEARNING GOALS

After completing this section, you will be able to:

- Describe how firewalls and gateways protect data.
- Identify ways to provide password protection.
- List safe hardware and software practices.
- Discuss how to combat viruses and other malware.
- Explain how to determine if websites are reliable.
- Prevent computer threats from public intrusion.

TERMS

gateway
passphrase
personal firewall
strong password
uninterruptable power supply (UPS)

Firewalls and Gateways

GS4 Living Online
2.1.4, 5.1.2

As discussed in Chapter 14, a firewall is a network device that blocks or allows certain kinds of network traffic. This forms a barrier between trusted and distrusted networks. Regardless of whether it is a software or hardware firewall, its purpose is to ignore data that come from unknown, unsecured, or suspicious locations.

Conventional firewalls protect computer networks. A **personal firewall** controls traffic to an individual machine. This type of firewall may control communication based on preset security instructions for specific software programs. This helps defend against malware trying to install executable programs on the individual machine.

For example, a computer may be protected by a hardware firewall while it is in the office. There it is linked to the Internet through the internal routers and servers. However, if the computer is a laptop taken outside of the office, it will not be protected by the hardware firewall. A personal firewall should be installed to protect the computer when it is used outside of the office, such as in airports and hotels.

Another way to protect a mobile computer is to rely on a hardware firewall that comes as part of a home-based router. This is not very expensive, but it must be activated and configured. It is also only available when you are at home. A separate device can be purchased to attach to the computer while on the road. These tend to be expensive.

A computer **gateway** is a device that joins two networks, as shown in Figure 16-9. For example, a gateway may connect a school's internal network to the Internet. A router is an example of a gateway device. It decides where data packets are to be sent based on an IP address.

FYI

If a laptop is connected through a VPN, it will be protected by the network's hardware firewall.

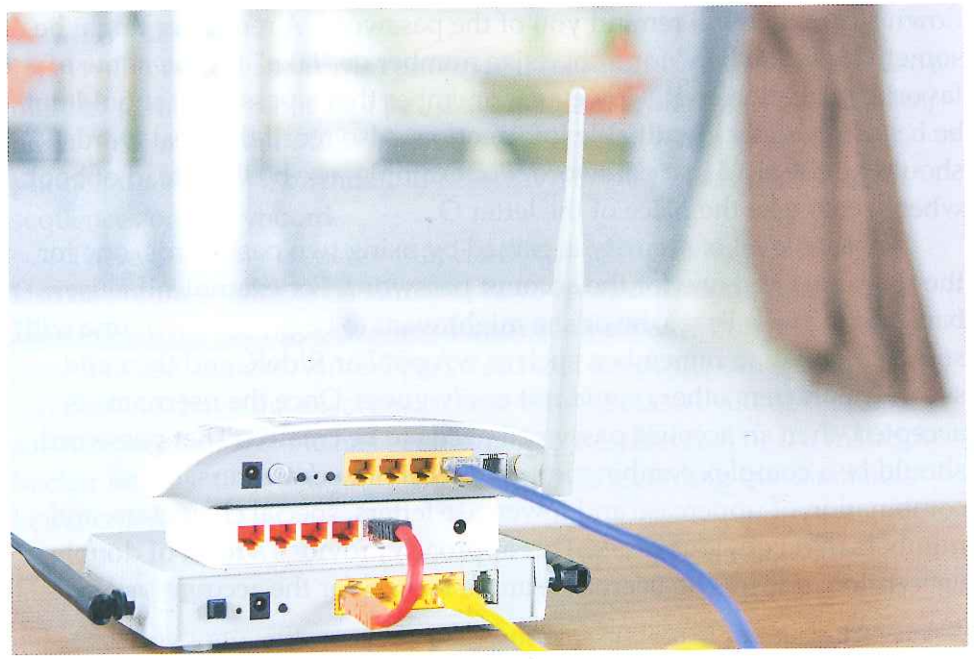

Sorapop Udomsri/Shutterstock.com

Figure 16-9. Routers are gateway devices because they determine where data packets are sent based on the IP addresses.

For small networks, there is little practical difference between a gateway and a firewall. In many cases, the functions of a gateway and a firewall are contained in a single unit. However, there are also dedicated versions of each device for use in large networks.

Most operating systems come with a firewall for protection. However, many computer users choose to install a commercial antivirus and antimalware program that includes a firewall, such as Norton Antivirus or McAfee Personal Firewall. Firewalls are also automatically available in popular routers, such as TP-LINK Archer C7 AC1750 Dual Band Wireless AC Gigabit Router.

GS5 Computing Fundamentals 7.6

Firewall settings can be manually changed. However, more often settings are automatically changed by regular updates to the firewall or OS. If a computer is connected to the Internet, it should never be run without a firewall or with the firewall disabled.

To manually modify the Windows firewall, open the Control Panel. Click the **System and Security** link, and then click the **Windows Firewall** link. The page that is displayed lists the current status of the firewall. To allow a specific program or feature through the firewall, click the "allow" link on the left. On the new page, click the **Change settings** button, and then click the **Allow another app...** button. A window is displayed in which you can browse for the application to allow through the firewall.

The settings for the firewall in a router can also be changed. Consult the owner's manual for the router for specific information on doing so.

GS5 Computing Fundamentals 7.1.2

GS4 Living Online 5.1.1

Password Protection

Never write down a password or leave obvious password hints near the computer. A sticky note with your password in plain site or even hidden under the keyboard or mouse pad is easy to find. Instead, write down a clue that will remind you of the password. A reminder might be something like "shoe" for a shoe size number or "lake" for the name of a favorite recreation spot. However, remember that a password should not be based on easily identifiable information. Also recall that real words should not be used in a password. For example, use b00k instead of book, where zeros take the place of the letter O.

Another level of security is gained by using two passwords, one for the username and one for the account password. For example, if a user banks with Wells Fargo, he or she might want to begin the username with something easy to remember, such as wAg@N or R!deR, and then add several characters others could not easily guess. Once the username is accepted, then an account password needs to be created. That password should be a complex combination of at least nine characters. Use a combination of uppercase and lowercase letters, special characters, and numbers in no obvious order. This approach provides a form of double encryption, one for the username and a second for the account password.

Password Management

In today's world, most people have many passwords to remember, and each password should be unique. Some people create a document file to store all of their passwords. If you choose to do this, do not name the file "Password," "Pass," or "PW." A hacker who gains access to the computer can easily search for such obvious file names. Instead of using a document file to store passwords, dedicated password-management software can be used. This type of software provides more security than a simple document file. Password-management software is readily available and can be quickly located by performing an Internet search.

GS5 Computing Fundamentals 7.1.2.1

Strong Passwords

In theory, every password can be cracked if given enough time. The goal is to make the password so difficult to crack that even a dedicated hacker will spend his or her time elsewhere. A **strong password** is one difficult for both humans and computers to crack. A strong password takes much more time to crack than a weak password. Strong passwords do not include real words, consecutive characters (aaa or ##), sequential characters (abc or 678), or common keyboard patterns (@#$% or rdxtfc).

- Develop a mnemonic device for remembering complex passwords.
- Use a combination of letters, numbers, and special characters.
- Use both lowercase and uppercase (capital) letters.
- Use passphrases you can memorize.
- Use different passwords on different systems.
- Do not create passwords based on personal information that can be easily accessed or guessed.
- Do not use words that can be found in a dictionary of any language.

FYI

Reusing the same password or varying it very little when changing it are frequent errors.

Weak or bad passwords contain real words and names. Do not use a maiden name; the name of a pet, child, sibling, celebrity, or sports team; or the title of a song or film. Bad passwords often relate to an address, phone number, SSN, birthday, anniversary, license plate, bank PIN, or sequences on a keyboard.

There are many websites that check the strength of a password. Use one of these sites to be sure you have created a strong password. However, when using such sites, do not enter a password you actually intend to use. Instead, enter a password that keeps the same structure, but does not have the exact characters. Why? Because you never know for sure whether the site has been spoofed (misdirected) or if a malicious hacker has installed a keystroke logger that is recording the characters being entered.

GS5 Computing Fundamentals 7.1.2.1

Passphrases

Creating long and complex passwords is standard practice. However, these are often hard to remember. A passphrase that is easy to remember can be used to create a password. A **passphrase** is a phrase composed of real words on which a password is based. For example, consider this passphrase: We often ate fish at 6:00 on Fridays? It does not use the real names of people or pets. It is fairly long and complex, but it is also relatively easy to remember. The password created from this passphrase may be: WeOf8F@60F?. This password is strong, which will take a long time to crack. The goal of creating a password from a passphrase is to make the password very hard to crack, but very easy to remember.

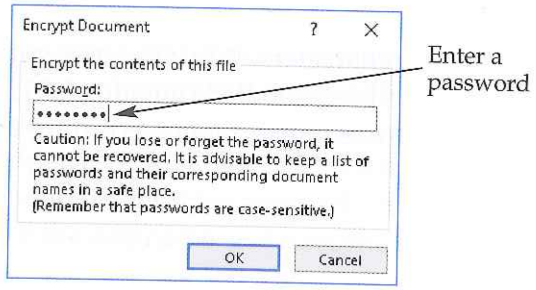
Passwords for Documents

A Microsoft Word document can be protected by using a password. The password is case-sensitive. Also, if you lose or forget a password, Word cannot recover your data. To password-protect a Word 2013 document, use this procedure. The procedure may be different depending on which version of Word you have.

1. Click the **File** tab.
2. Click **Info** on the left-hand side of the backstage view.
3. Click the **Protect Document** button on the right-hand side of the backstage view, and then click **Encrypt with Password** in the drop-down menu that is displayed.
4. In the **Encrypt Document** dialog box, enter a password, and then click the **OK** button, as shown in Figure 16-10.
5. In the **Confirm Password** box, enter the password again, and then click the **OK** button. A message appears in the backstage view indicating that a password is now required to open the document.

Microsoft Excel provides several ways to protect a workbook. The user can require a password to open and view the file, a password to change data in the file, and even a password to add, delete, or hide worksheets. The basic approach to adding a password for the workbook structure in Excel 2013 is as follows. The procedure may be different depending on which version of Excel you have.

1. Click the **File** tab.
2. Click **Info** on the left-hand side of the backstage view.
3. Click the **Protect Document** button on the right-hand side of the backstage view, and then click **Protect Workbook Structure** in the drop-down menu that is displayed.



Encrypt Document

Encrypt the contents of this file

Password:

••••••••

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place.
(Remember that passwords are case-sensitive.)

Enter a password

Goodheart-Willcox Publisher

Figure 16-10. Enter a password to protect the document.

STEM

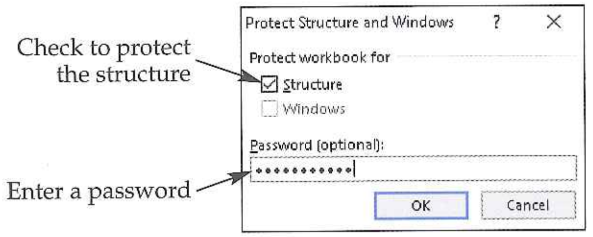
Mathematics

To multiply decimals, place the numbers in a vertical list. Then multiply each digit of the top number by the right-hand bottom number. Multiply each digit of the top number by the bottom number in the tens position. Place the result on a second line and add a zero to the end of the number. Add the total number of decimal places in both numbers you are multiplying. This will be the number of decimal places in your answer.

FYI

Password-protecting a Microsoft Office document does not encrypt the file, which means that hackers may still be able to crack the data.

4. In the **Protect Structure and Windows** dialog box, enter a password, check the **Structure** check box, and then click the **OK** button, as shown in Figure 16-11.
5. In the **Confirm Password** box, enter the password again, and then click the **OK** button. Now, worksheets cannot be added, deleted, or moved.
6. Click the **File** tab, and then click **Info** on the left-hand side of the backstage view. A message appears in the backstage view indicating that the structure cannot be changed.



Protect Structure and Windows

Protect workbook for

☑ Structure

□ Windows

Password (optional):

•••••••••••

Check to protect the structure

Enter a password

Goodheart-Willcox Publisher

Figure 16-11. When protecting the structure of an Excel workbook, a password can be entered.

Password Use

The way in which passwords are used is as important as how they were created. Even a strong password cannot protect a device if a cyber criminal can easily access it. The following habits will help further protect strong passwords.

- Never disclose or share the password with anyone.
- Do not use the same password for multiple accounts.
- Change passwords on a regular basis.
- Use a very strong password to protect a document that contains a list of other passwords.
- Immediately change *all* of your passwords if you detect suspicious activity on *any* of your accounts.

Hands-On Example 16.3.1

Strong Passwords

The first line of defense to protecting data is a strong password. There are many websites that will check the strength of a password, many for free.

1. Launch a browser, and navigate to a search engine.
2. Enter the search phrase Microsoft password checker.
3. Click the link for the Microsoft password checker website. It should be at the top or very near the top of the list. Notice that this is a secure web page.
4. Enter a password to see its strength.
5. Vary the length of the password, the characters used, and position of characters within the password to see how the strength of the password changes.
6. Enter a password based on this passphrase: My teacher is great! One example is m1T3chRisGr8!

Safe Hardware and Software Practices

Simply having good hardware and software is not enough to provide cybersecurity. You are responsible for knowing how to properly use what has been purchased and installed. You are also responsible for remaining alert and acting responsibly whenever connected to the Internet. Regardless of precautions taken, every computer user can expect to end up trying to open a corrupted file. Even worse, you may be faced with trying to work on a computer that has been infected with a virus.

MAii Thitikorn/Shutterstock.com

Figure 16-12. A UPS provides a constant supply of power to the computer in case of a power outage. It protects the computer against power surges and prevents data loss during storms.

UPS, System Restore Backup Points, and Individual File Backups

An **uninterruptable power supply (UPS)** is a device that protects computer systems and files against power surges and outages, as shown in Figure 16-12. Electronic equipment should be unplugged during thunderstorms. A UPS can provide power while the system is unplugged or if the building loses power. A UPS also protects the system if there is an electrical surge. An electrical surge can damage or destroy electronic equipment.

Even when file damage has occurred, all is not lost if a system restore point has been established and back-up files have been created. Backups of document files should be made on a flash drive, an external drive, or a cloud-storage site. This subject is discussed in more detail in Chapter 4.

Maintenance Schedule

The operating system and programs on your computer have many security features. However, these features are exactly what hackers and malware try to crack. Therefore, experts suggest reevaluating a computer's security setup at least twice a year. Pick two dates that are easy to remember, such as New Year's Day and the Fourth of July or when daylight saving time starts and stops.

Regularly review the settings associated with the applications on your computers. Browser software, in particular, has security settings in its list of preferences. Each program is a little different, so look for commands such as **Privacy**, **Safety**, and **Security**. Check the settings for deleting browsing history, accessing trusted sites, and blocking pop-up windows. Set the security level to high and save it.

FYI

When reviewing security settings, do not forget instant messaging software and social networking websites.

Offers of Free Software Protection

Most credible firewall and antivirus software solutions come as an annual subscription costing $50 or more. Such software must be legally licensed. However, it is common to see offers of free software of this type when online. Most of these offers are bogus and may, in fact, be spreading malware.

Legitimate Free Software

There is some legitimate free antivirus software. These programs are distributed as shareware, even if they are not called that. The best features are either limited or disabled. The providers hope you will upgrade to the deluxe or professional edition to unlock these features. However, the upgrade is not free. There are some fully functional and completely free antivirus programs. Some of these are open-source software.

Free PC Scans

Many of the offers of free software protection come as "free PC scans." These offers often pop up when you surf the Internet. The popup may announce that your system or files have been corrupted and then offers a free security scan or a free service to speed up your machine. These offers are likely to be scams. One company had to pay a $1 million fine for offering "free spyware scans" that told users their systems had been infected even when the systems were entirely clean. Some "scans" do more than give misleading results. They actually try to install malware on your computer.

Many of these pop-up ads do not have a way to be closed. The only button the user sees is a **Scan** button. Do not click this button. The safest approach is to close the browser window. Pop-up blocker software will prevent many of these ads from appearing.

Combating Viruses and Other Malware

GS5 Computing Fundamentals 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.5.1

GS4 Computing Fundamentals 3.4.4, 4.1.3
Living Online 5.1.2

Over 40,000 computer viruses have been identified, and they come in many varieties. Here are some common types:

- Boot sector malware infects only the DOS boot sector.
- Backdoor malware creates a software hole in the computer that can be used by hackers as an open door.
- Trojan horse is a seemingly harmless file that unleashes malicious code to tear down a computer's defenses.
- Rootkit is malware that not only infects a computer, but also fights back by restarting or moving itself when a removal attempt is made.

Antivirus software can block virus transmissions and repair damage caused by viruses. In order for it to be most effective, the software needs to be updated on a regular basis.

Block Virus Transmission

Computer viruses can be transmitted in many ways. They may be loaded via CDs and flash drives. They may be hidden in the subject line or body of e-mail messages, activated by clicking on an object or attachment, and even activated by replying to a message. They can be downloaded from many locations on the Internet.

When a virus is suspected in an e-mail, the best approach is to delete the e-mail. Do not open it. If you have already opened it, do not click on any of the content. Immediately close the message, and then delete it. If you suspect an Internet site of transmitting a virus, immediately close the browser.

Always have your antivirus software running. Most antivirus software will actively try to prevent malware from being transmitted to your computer. Some antivirus software will also prescreen Internet sites for potential dangers. If your antivirus software warns against opening a site, do not open the site. Additionally, most antivirus software can be set to run a scan on a regular basis. If this is an option, schedule a scan at least once a week. If the software does not allow scans to be scheduled, manually run a scan on a regular basis.

Repair Virus Damage

If your computer seems unusually slow or your web browser suddenly looks different, your computer may have a virus. Viruses may make a computer unstable, causing it to crash fairly often. If a virus has infected a file you are trying to open, you may receive a message saying the file has been corrupted and cannot be opened.

The first step in repairing virus damage is to run a scan using your antivirus software. Follow the instructions in the software. In some cases, the malware is severe and the computer will not function. If the computer is not functioning, turn it off and seek expert assistance.

GS5 Computing Fundamentals 7.5.2

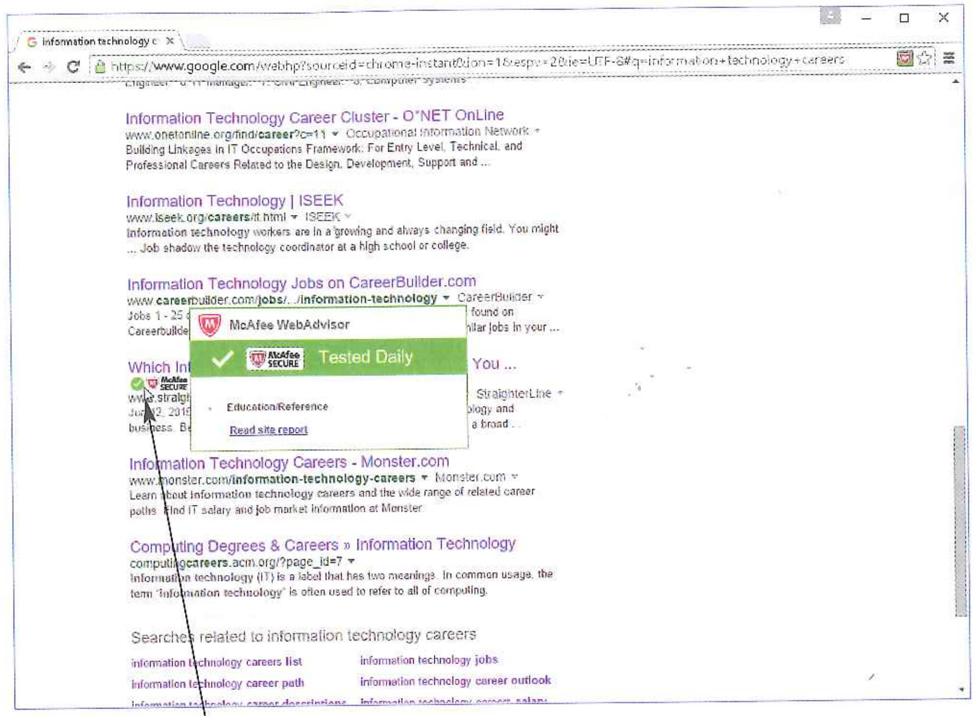
Keep Antivirus Software Updated

Always update your operating system and antivirus software with the latest security patches. Doing so offers excellent protection against any hacker attempts to download or execute code on your computer. Always use a well-established and modern web browser. The most current browsers provide protection against malicious activity and warn of sites known to exhibit malicious behavior. Antivirus software often works with search engines to let the user know of safe and unsafe sites, as shown in Figure 16-13.

Most antivirus software automatically checks for updates every few days when you are connected to the Internet. If you have not been on the Internet for some time, it is a good idea to manually update the antivirus software. Do this before navigating to any Internet sites or checking e-mail. If the software does not automatically check for updates, be sure to manually update it every few days.

FYI

Do not expect to increase security by loading more than one antivirus program. Most antivirus software does not work well with other antivirus software.


information technology c ×
https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=information+technology+careers

Information Technology Career Cluster - O*NET OnLine
www.onetonline.org/find/career?c=11 ▾ Occupational Information Network ▾
Building Linkages in IT Occupations Framework: For Entry Level, Technical, and Professional Careers Related to the Design, Development, Support and ...

Information Technology | ISEEK
www.iseek.org/careers/it.html ▾ ISEEK ▾
Information technology workers are in a growing and always changing field. You might ... Job shadow the technology coordinator at a high school or college.

Information Technology Jobs on CareerBuilder.com
www.careerbuilder.com/jobs/.../information-technology ▾ CareerBuilder ▾
Jobs 1 - 25 ... found on Careerbuilde... ...ilar jobs in your ...

McAfee WebAdvisor
✓ McAfee SECURE Tested Daily
Education/Reference
Read site report

Which Inf... You ...
McAfee SECURE
www.straigh... StraighterLine ▾
Jun 2, 201... ...ology and business. B... a broad ...

Information Technology Careers - Monster.com
www.monster.com/information-technology-careers ▾ Monster.com ▾
Learn about information technology careers and the wide range of related career paths. Find IT salary and job market information at Monster.

Computing Degrees & Careers » Information Technology
computingcareers.acm.org/?page_id=7 ▾
Information technology (IT) is a label that has two meanings. In common usage, the term 'information technology' is often used to refer to all of computing.

Searches related to information technology careers
information technology careers list | information technology jobs
information technology career path | information technology career outlook

Hover to display the message

Goodheart-Willcox Publisher

Figure 16-13. Some antivirus software will work with search engines to prescreen results. In this example, green check marks indicate sites without any reported problems, and hovering the cursor over a check mark displays the message.

Hands-On Example 16.3.2

Antivirus Software

Antivirus software is an important part of cybersecurity. Before purchasing antivirus software, it is a good idea to research the different programs that are available.

1. Launch a browser, and navigate to a search engine.
2. Enter these keywords: best antivirus software ratings.
3. In the search results, look for a link from a computer magazine such as PC Magazine or PC World that is a review of antivirus software. A link for Consumer's Report that provides a review is also a good choice.
4. Click the link, and review the current ratings and prices. Ratings and prices will vary by source. Most software is usually between $50 and $100 for a one-year subscription. However, some software offers a free version with basic features with premium features available in a subscription version.
5. Select an antivirus software you feel would best meet your needs. Write one paragraph justifying your choice.

GS4 Living Online
5.1.1, 5.1.2

Determining Reliable Websites

How can you know a website can be reliably used without picking up a virus? Unfortunately, there are no iron-clad guarantees. Some of the most famous and secure websites have been hacked. However, there are a number of ways to greatly reduce the risks of downloading a virus.

The safest way to navigate to a site is to manually enter the URL. Clicking a link to the site on another web page could send you to a fake site. If the link is in an e-mail from an unknown sender, delete the e-mail. That is a very common method for getting people to go to virus-infected sites.

Check the domain name to see if it is a typically reliable domain. Governmental (.gov) and educational (.edu) domains are usually safe and reliable. These domains are not available to the general public. However, many educational institutions provide their students with .edu e-mail addresses or web space. Student accounts are often not as closely monitored as the school's main sites. Therefore, they may present the risk of malware.

FYI

Many risky websites have a very professional appearance. Just because a site appears well-developed does not mean it is safe.

Look at the structure and appearance of the website. If it is very basic and poorly designed, it may pose a risk. The site may be intentionally passing along malware or it may contain files infected due to carelessness. Look for misspellings and grammar errors, broken links, and elements that overlap or are otherwise improperly formatted. If the site is complex and appears to have been built over many years by dedicated programmers, it is more likely to be a safe site.

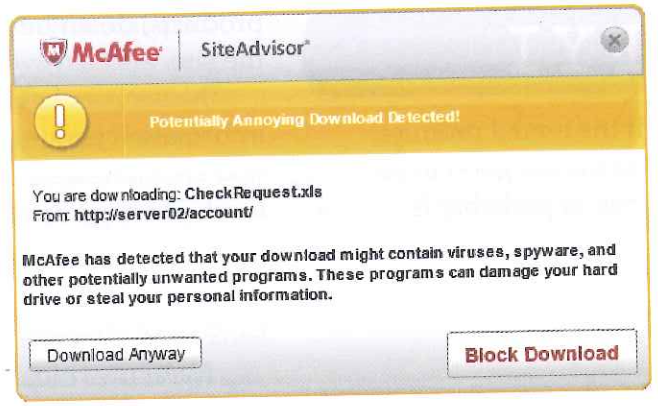
Before going to a site, enter the site name into a search engine along with the word "complaint." If there are problems with the site, there will likely be many complaints. For example, compare results from entering "Win 7 Antivirus 2012" or "24x7 help" with results from entering "XP patches." If many Internet users agree a site is unsafe, do not go to the site.

Safe File Downloads

In the rapidly changing cyber war, any file could be potentially unsafe. However, there are some questions you can ask to help decide if the file is likely safe or unsafe.

- Have you successfully used the site before?
- Is the site a governmental site?
- Does the site name or invitation to download look suspicious?
- Does the site or file have a digital logo or signature?
- Does your antivirus software warn about the site or the file?
- Do you have sufficient time to download the file without interruption?
- Can the file be downloaded to a separate drive and tested there before installing it on your main computer?

Be particularly wary of certain file types, such as those with these file extensions: .bat, .com, .exe, .pif, and .scr. These files are executable files that run programs, which may be malware. Carefully check the source to make sure you trust it before downloading the file. Remember, a file can only have one file name extension. If a file appears to have two file name extensions, such as readme.txt.exe, only the last one is the actual extension. This is an attempt to make the user think the file is safe, but it likely contains malware. Also, most antivirus software will warn of a potentially dangerous download before allowing it, as shown in Figure 16-14.



You are dow nloading: CheckRequest.xls
From: http://server02/account/

McAfee has detected that your download might contain viruses, spyware, and other potentially unwanted programs. These programs can damage your hard drive or steal your personal information.

Goodheart-Willcox Publisher

Figure 16-14. Most antivirus software will warn of a potentially dangerous download and ask the user to block or verify the download.

Consider the topic of the file being downloaded. If the topic of the file appears illegal or suspicious, the file may be dangerous. If the offer seems too good to be true, then there may be a high risk the downloaded file contains malware. However, if the file concerns a bill for cleaning streams in upstate New York, for example, the risk may be low because the audience is limited. Hackers usually focus on areas of high interest, such as offers of free photographs, software, or financial advice.

FYI

Entering the file name into a search engine may return results indicating an unsafe file.

GS4 Living Online
5.1.1

Internet Scams or Fraudulent Websites

Criminals think of clever ways to separate you from hard-earned cash. Check for Internet phishing scams or fraudulent websites. New ones are created daily. Many Internet users turn to Snopes (www.snopes.com) to check out a wide variety of rumors, phishing scams, and websites that mimic or spoof reliable sites. Snopes examines the evidence behind popular Internet and e-mail stories and evaluates whether they are real or fake.

Beware of e-mail about a security concern from your bank or an e-commerce site. Be very cautious of any "urgent" e-mail request to provide or update your personal information. Any link in the e-mail almost certainly goes to a website that is phishing for data or transmitting malware. Never be fooled by e-mail telling sad stories, making unsolicited job offers, or promising lottery winnings. These are almost always Internet scams.

E-commerce Sites

Many people make purchases on e-commerce websites. However, e-commerce sites pose some risks. Since the buyer cannot see or touch the goods offered for sale, there is no way to see if the product is of poor quality. There are many online e-commerce sites that offer prescription medications. Some of these offer medications that are not manufactured under the regulations of the Food and Drug Administration (FDA). These medications may be of poor quality or, in some cases, completely fake. Additionally, a website may be *presented* as an e-commerce site, but its real purpose is to attract people to enter credit card details. Unless shopping on a well-known site with a reputation of providing quality

FYI

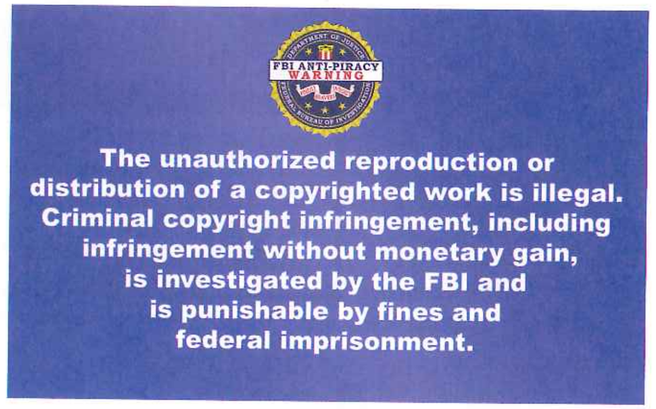
If the e-mail promise seems too good to be true, it probably is. Ignore the offer and delete the e-mail.

products, do an Internet search to discover comments on the reputation of the site.

Never purchase anything from a spammer. If you did not request information about a service or product, it is almost certainly a scam. If you are interested in the product or service, manually search the Internet for it. Then, go directly to the legitimate source. Do not use the links provided in the spam e-mail.

Pirated Media

Never download pirated media, such as songs, movies, software, or anything else. Not only is doing so illegal, it is a good way to download malware. The idea of viewing a hot new movie or expanding your music library by downloading the current hits for free is appealing. Free file-sharing sites and services are a prime way for a computer to become infected with malware. No movie or song is worth corrupting your machine or the fines and prison time you face by downloading pirated media, as shown in Figure 16-15.


FBI ANTI-PIRACY WARNING

The unauthorized reproduction or distribution of a copyrighted work is illegal. Criminal copyright infringement, including infringement without monetary gain, is investigated by the FBI and is punishable by fines and federal imprisonment.

Goodheart-Willcox Publisher

Figure 16-15. Pirating songs, movies, software, or anything else is illegal and carries a harsh penalty.

Preventing Threats from Public Intrusion

External threats can come from individuals, criminal groups, or foreign governments. The "enemy" may disclose, modify, or destroy your information. Vulnerabilities may be caused by poor software coding or by weak administrative controls.

Peer-to-Peer File Sharing

Do not use peer-to-peer (P2P) file sharing. There is nothing illegal about sharing photographs you take with family and friends. However, many authorities believe that P2P file sharing is mostly used to share illegal content, such as a copyrighted material. Furthermore, becoming part of the P2P network puts your computer at increased risk. Your computer becomes open to viruses, spyware, and other threats.

Public Internet Providers

Conducting any business on shared public Internet providers can be very dangerous. Public Internet providers, or hotspots, are common at airports, hotels, Internet cafés, libraries, and other public places. However, these networks do not provide a secure connection. They are not password-protected. Hackers may be using key-logger software to capture everything entered on the hotspot. Scammers may also be using their cell phone cameras to watch as login, password, or account information is being entered.

Some people have devices that provide their own mobile hotspot. Sometimes these are not password-protected. This allows hackers easy access. Additionally, it may be tempting to take advantage of somebody who has not password-protected his or her hotspot to get free Internet access yourself. However, doing so grants easy access to *your* data.

Access Security

GS4 Living Online 2.1.3

Computer-network connections cannot be guaranteed to be totally secure. Wireless connections are less secure than wired connections. This is because no physical access is required by the hacker. Even wired access does not guarantee security. The network administrator or others can tap into data flowing from individual computers to the router.

Public Wi-Fi hotspots and public-access computers are very convenient. They do not require passwords and there are many tasks that users can feel comfortable performing on open networks. You can browse the web, catch up on news stories, watch online videos, or listen to streaming music. However, these public sites are very vulnerable.

FYI

When creating a strong password, be sure it offers no hint of the location, your name, or other easily identifiable information.

Wireless Security

Computer equipment is commonly connected to the Internet via a wireless router. With wireless connections, security requires some form of data encryption between the computer and the wireless router. However, a wireless router that appears to be protected may be only using the factory-installed user name and password. These are very easy to guess or even to look up on the Internet.

Wireless signals can be easily intercepted. Therefore, it is important to secure the connection by setting a strong password for the router and using a complex router protocol. Whenever the option is available, it is best to use the WAP2 protocol. This requires a passphrase before connecting to the Internet for the first time. The previous router standard (WEP) should not be used. It can be cracked in less than a minute by common hacker software.

TITANS OF TECHNOLOGY

Debora A. Plunkett was Information Assurance Director at the National Security Agency (NSA) from 2010 until 2014, when she assumed another position within the NSA. She served as deputy director prior to her appointment as director. While serving as director, she was responsible for all of the national security systems for the United States. Those responsibilities covered vulnerability and threat assessments, cryptography, and spreading information about computer security. In 2007, she was awarded the rank of meritorious executive in the Senior Cryptologic Executive Service by the President of the United States. Beginning her career with the Baltimore City Police Department, Plunkett has used analytical skills developed there to respond to the growing threats of cybersecurity in her role at the national level.

Even if the Wi-Fi network requires a password or certificate to connect, it may still be possible for other people on the network or Internet to access your information unless the connection uses HTTPS. This encrypted connection is often indicated by a lock icon on the link or in the browser's address bar. A VPN can also be used to ensure a more secure, encrypted connection.

The wireless connection to the router within your home may not be secure. Your wireless signal can be "heard" a block or more away. For extra protection, install and use a software firewall on individual computers and devices.

Users of a public hotspot should try to make sure they are connecting to a legitimate hotspot. Hackers sometimes set up pirate routers with familiar names. The name, or identifier, for a wireless connection is known as service set identifiers (SSID).

GS5 Computing Fundamentals 7.4.3.3

Public Computers

Using a public computer, such as those found in libraries, is relatively safe for generalized surfing of the web. However, using one even for a simple task related to personal information, such as checking e-mail, can be quite risky. A hacker may have installed spyware to log keystrokes. It is especially important not to enter credit card information into a public computer.

Social networking sites, web-based mail sites, and e-commerce sites often include automatic log-in features that have been designed to save each user's name and password. If you need to use a public computer to log into one of these accounts, be sure to log out when done. It is not enough just to close the browser window. Even navigating to another site may not log you out of the account. Some browsers have a "private" or "anonymous" mode that allows you to browse the web without leaving a trace. If available, this feature should be used on a public computer.

Even low-tech methods may pose a risk while using a public computer. Someone nearby may be watching. While most password-entry text boxes do not show the actual password as it is entered, somebody could be watching your fingers.

Guidelines

When using public computers or unprotected hotspots, adhere to the following guidelines. Doing so will help increase the level of security.

- Do not opt to save any log-on information while using public computers.
- If you sign into a website, always log out of it.
- Completely log off the computer when finished with the session.
- Disable automatic login features on software or websites so no one can log in as you.
- Do not leave the computer unattended, even if it is your own computer.
- Enable "private" or "anonymous" browsing before entering personal data.

16.3 Section Review

Check Your Understanding

1. What are the characteristics of a strong password?
2. During a thunderstorm, what should be done to the computer?
3. What is the first step in repairing damage caused by a computer virus?
4. Which file types are executable files that can run programs?
5. Which wireless protocol should *not* be used?

IC3 Certification Practice

The following question is a sample of the types of questions presented on the IC3 exam.

1. Which of the following is the strongest password?
   A. User123
   B. B00kR3dr
   C. SpotTheDog
   D. 416MainSt

Build Your Vocabulary

As you progress through this course, develop a personal IT glossary. This will help you build your vocabulary and prepare you for a career. Write a definition for each of the following terms and add it to your IT glossary.

gateway
passphrase
personal firewall
strong password
uninterruptable power supply (UPS)

16 Review and Assessment

Chapter Summary

Section 16.1 Preventing Computer Threats

- Malware is software that intentionally performs actions to disrupt the operation of a computer system, collect private information, or otherwise harm the computer or user. Other computer threats come from phishing, data vandalism, cookies, and computer hacking.
- Internet protocols tell computers, modems, routers, and networks how to communicate with each other. There are several Internet protocols related to security, including TCP/IP, SSH, HTTPS, and others.
- The easiest way to protect information from corruption is by backing up those files in other locations. Data should be cleared from any computer equipment before it is recycled.

Section 16.2 Identity Protection and Ethical Behavior

- Identity theft is an illegal act that involves stealing someone's personal information and using that information to commit theft or fraud. To protect against this, security is important on LANs, WANs, VPNs, and wireless networks.
- Identity theft can occur via e-mail. Check questionable messages, be wary of attachments from unknown sources, do not click links in e-mail, and stay alert for phishing attempts.
- Ethics are the principles of what is right and wrong that help people make decisions. There are legal and ethical responsibilities for everything you do online.

Section 16.3 Restricting Access to Personal Information

- A personal firewall controls traffic to an individual machine, while a computer gateway is a device that joins two networks. A firewall forms a barrier between trusted and distrusted networks.
- A strong password is one difficult for both humans and computers to crack. Never disclose or share the password with anyone, and do not use the same password for multiple accounts.
- An uninterruptable power supply (UPS) is a device that protects computer systems and data files against power surges and outages. Backups should be made and maintenance should be used to further protect against data loss.
- There are thousands of computer viruses, and they can be transmitted in various ways. Keep antivirus software up to date, but if a virus cannot be blocked, its damage must be repaired.
- There are no iron-clad guarantees to ensure a website is safe, but take precautions to see if the site is reliable, such as checking the domain. Do not download any file if you suspect it to be unsafe, and *never* download pirated media.
- External computer threats can come from individuals, criminal groups, or foreign governments. Do not use P2P file sharing sites, and avoid using public Internet providers and unsecured personal hotspots.

Now that you have finished this chapter, see what you know about information technology by scanning the QR code to take the chapter posttest. If you do not have a smartphone, visit www.g-wlearning.com.

Chapter 16 Test

Multiple Choice

Select the best response.

1. Which of the following is *not* a major computer threat?
   A. hackers
   B. corrupted files
   C. malware
   D. CAPTCHA
2. How can hacking be legitimate?
   A. Hiring a hacker to find security flaws in a competitor's computer system.
   B. Hiring a hacker to find security flaws in your computer system.
   C. Hacking into a social media website to remove your personal data.
   D. Hacking is never legitimate.
3. Which of the following is *not* a safe practice to deter identity theft?
   A. Set social networking profiles to public.
   B. Immediately delete messages from suspicious senders.
   C. Never click any links in unsolicited e-mail.
   D. Ensure that the lock symbol is shown in your browser's status bar.
4. WeOf8F@60F is an example of what?
   A. short password
   B. gateway logon
   C. wireless firewall code
   D. passphrase password
5. What is the function of a firewall in a network?
   A. Join two networks.
   B. Block some network traffic.
   C. Reduce temperature of internal components.
   D. Set port IDs for WANs and LANs.

Completion

Complete the following sentences with the correct word(s).

6. _____ encrypts files or blocks the user's access to programs until the user pays to unlock them.
7. The _____ is a network protocol that secures data communication and remote command execution.
8. Websites that you must join, such as Facebook and Twitter, have _____ that explain what can be posted or shared.
9. A computer _____ is a device that joins two networks.
10. A(n) _____ is a phrase composed of real words on which a password is based.

Matching

Match the correct term with its definition.

A. Trojan horse
B. cookie
C. pharming
D. online piracy
E. strong password

11. Downloading copyrighted material without permission of the copyright holder.

12. Virus or other malware infects the computer and takes control of your web browser.
13. Program that invites the user to run it while concealing malicious code that will be executed.
14. Small text files placed on a computer's hard disk by a website.
15. Difficult for both humans and computers to crack.

Application and Extension of Knowledge

1. Locate three different websites that check the strength of a password. Evaluate each site for validity and relevance. Write one paragraph for each site describing the site, providing the URL, and explaining why you believe the site to be safe.
2. Identify five applications of passwords in your personal life. These may be your cell phone, your computer, online gaming websites, social media sites, or anything that requires a password. Research the password requirements for each. Identify which characters are allowed, if there is a minimum length, and any other requirement. Make a table or chart to compare the requirements.
3. Create five passwords for the applications identified in #2. Be sure each meets the requirements you identified for the application. Also be sure to apply the guidelines provided in this chapter.
4. Using the three websites you identified in #1, check the strength of each password you created in #3. Check each password on each website. If any password does not pass any of the website tests, modify the password until it does pass all three.
5. Create a passphrase and password for a gaming website. Do not create ones you actually want to use. Prepare a presentation for the class identifying the passphrase and password. Explain why you created the passphrase and how you turned it into a password.

Online Activities

Complete the following activities, which will help you learn, practice, and expand your knowledge and skills.

Certification Practice. Complete the certification practice test for this chapter.

Vocabulary. Practice vocabulary for this chapter using the e-flash cards, matching activity, and vocabulary game until you are able to recognize their meanings.

Communication Skills

College and Career Readiness

Writing. Generate ideas that relate to the importance of accurate information. Make a list of reasons you would provide when explaining to a coworker why accurate information is important in each form or communication that is completed in a business situation.

Listening. Hearing is a physical process. Listening combines hearing with evaluation. Effective leaders learn how to listen to their team members. Listen to your instructor as the material in this chapter is presented. Listen carefully and take notes about the main points. Then, organize the key information that you heard. What points would you reiterate if you were presenting the chapter?

Speaking. Participate in a one-on-one communication with a classmate about the benefits of using electronic filing for personal income tax. Keep in mind that your style of presentation can influence the opinion of the listener.

Internet Research

Internet Security and Ethical Use. Using the Internet, research the laws that relate to Internet security. When were they created? What is their purpose? Next, research laws regulating hacking and browser hijacking. Summarize what you learned about Internet security and ethical conduct.

Teamwork

Learning to work effectively in a team environment will be an asset in your career and personal life. Exhibiting positive interpersonal skills, as well as critical thinking skills, to solve problems or assignments can make you a productive individual. Working with your team, create a list of standards for safety in your classroom as well as personal safety standards for individual well-being. Present your ideas to the class and how these standards can be implemented.

Portfolio Development

College and Career Readiness

Organizing Your Portfolio. You have collected various items for your portfolio and tracked them in your master spreadsheet. Now is the time to organize the contents. Review the items and select the ones you want to include in your final portfolio. There may be documents that you decide not to use. Next, create a flowchart to lay out the organization for your portfolio. Your instructor may have specific guidelines for you to follow.

1. Review the documents you have collected. Select the items you want to include in your portfolio.
2. Check the quality of each item in your folders. Make sure that the documents you scanned are clear. Do a final check of the documents you created to make sure they are high quality in form and format.
3. Create the flowchart. Revise until you have an order that is appropriate for the purpose of the portfolio.

CTSOs

EVENT PREP

Day of the Event. You have practiced all year for this CTSO competition, and now you are ready. Whether it is for an objective test, written test, report, or presentation, you have done your homework and are ready to shine. To prepare for the day of the event, complete the following activities.

1. Get plenty of sleep the night before the event so that you are rested and ready to go.
2. Use your event checklist before you go into the presentation so that you do not forget any of your materials that are needed for the event.
3. Find the room where the competition will take place and arrive early. If you are late and the door is closed, you will be disqualified.
4. If you are making a presentation before a panel of judges, practice what you are going to say when you are called on. State your name, your school, and any other information that will be requested. Be confident, smile, and make eye contact with the judges.
5. When the event is finished, thank the judges for their time.